Method and device for coding useful data

Patent Number: DE3631797
Publication date: 1988-03-31
Inventor(s): SCHMIDTKE FRANK (DE)
Applicant(s):: SIEMENS AG (DE)
Requested Patent: DE3631797
Application Number: DE19863631797 19860918
Priority Number(s): DE19863631797 19860918
IPC Classification: H04L9/00 ; G09C1/00
EC Classification: H04L9/00
Equivalents:

Abstract

A pair of keys consisting of a secret key and a public key (KGA, KGB, KPA, KPB) is in each case allocated to a first and second communications terminal (A, B). The first communications terminal (A) generates a first temporary key common to both communications terminals (A, B) as random number (KS1) and from this a first temporary key (KSA1) with its public key (KPA) in accordance with an asymmetric coding method, and a second temporary key (KSB1) with the public key (KPB) and (B). The first communications terminal (A) generates the first temporary key (KS1) common to both communications terminals (A, B) with its secret key (KGA) and the first temporary key (KSA1), by means of which common temporary key it codes first useful data (ND1) in accordance with a symmetric coding method. It transmits the second temporary key (KSB1) and the first coded useful data (ND1') to the second communications terminal (B) which decodes the second temporary key (KSB1) with its own secret key (KGB) and by this means forms the first temporary key (KS1) common to the two communications terminals (A, B), by means of which common first temporary key it then decodes the transmitted coded first useful data (ND1').

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 36 31 797 C2**

(51) Int. Cl.[5]:
H 04 L 9/00
G 09 C 1/00

(21) Aktenzeichen: P 36 31 797.7-31
(22) Anmeldetag: 18. 9. 86
(43) Offenlegungstag: 31. 3. 88
(45) Veröffentlichungstag der Patenterteilung: 22. 10. 92

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 1000 Berlin und 8000 München, DE

(72) Erfinder:
Schmidtke, Frank, 8000 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US-Z.: ZIMMERMANN, P: A proposed standard format for RSA crypto-systems. In: Computer, Nr. 9, Sept. 1986, S. 21-34;
DE-B.: WECK, G.: Datensicherheit, Stuttgart, B.G. Teubner, 1984, S. 290-295;

(54) Verfahren und Vorrichtung zur Verschlüsselung von Nutzdaten

DE 36 31 797 C2

DE 36 31 797 C2

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Verschlüsselung von Nutzdaten, die zwischen einer ersten und zweiten Kommunikationsendstelle (A, B) übertragen werden, denen jeweils ein aus einem geheimen und einem öffentlichen Schlüssel (K_{GA}, K_{GB}, K_{PA}, K_{PB}) bestehendes Schlüsselpaar zugeordnet ist.

Es sind bereits verschiedene Verfahren zur Verschlüsselung von Nutzdaten bekannt. Ziel der Verschlüsselungsverfahren ist es, die Nutzdaten in einer solchen Weise einer mathematischen Transformation zu unterwerfen, daß es einem Unbefugten nicht möglich ist, die Originaldaten aus den transformierten Daten zu rekonstruieren. Dabei muß es für den legalen Empfänger der transformierten Daten möglich sein, durch Anwendung einer inversen Transformation aus den verschlüsselten Daten wieder die Originaldaten zu regenerieren. Die mathematische Transformation wird üblicherweise mit Verschlüsselung und die inverse Transformation mit Entschlüsselung bezeichnet.

Die bekannten Verschlüsselungsverfahren lassen sich in symmetrische und asymmetrische Verschlüsselungsverfahren unterteilen. Bei symmetrischer oder sogenannter konventioneller Verschlüsselung werden bei der Verschlüsselung und bei der Entschlüsselung identische Schlüssel verwendet. Zu den symmetrischen Verschlüsselungsverfahren gehört das sogenannte DES(Data Encryption Standard)-Verschlüsselungsverfahren bei dem jeweils 64 Bit des Klartextes unter Verwendung eines für die Verschlüsselung des gesamten Klartextes gültigen Schlüssels von 56 Bit Länge in 64 Bit Schlüsseltext umgesetzt werden.

Das DES-Verschlüsselungsverfahren ist ausführlich von D. E. Denning, Cryptography and Data Security, Addison Wesley, Reading, Mass, 1983; von W. Davies, W. L. Price, Security for Computer Networks, John Wiley & Sons, 1984 und G. Weck, Datensicherheit, Maßnahmen und Auswirkungen des Schutzes von Informationen, B. G. Teubner Stuttgart 1984, Seiten 290—295 beschrieben. Mit symmetrischen Verschlüsselungsverfahren läßt sich ein hoher Durchsatz der zu verschlüsselnden Nutzdaten erzielen (mehr als 10 Kbit/s), da der erforderliche Rechenaufwand relativ gering ist. Als problematisch erweist sich jedoch die Übertragung des von beiden Kommunikationspartnern gemeinsam zu verwendenden Schlüssels.

Die asymmetrischen Verschlüsselungsverfahren beruhen auf Algorithmen, die eine Ver- und Entschlüsselung mit unterschiedlichen, nicht auseinander ableitbaren Schlüsseln ermöglichen. Zu dieser Verfahrensgruppe gehört das sogenannte RSA-Verfahren, das von R. L. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Comm. of the ACM, 21, No. 2, 1978 ausführlich beschrieben ist. Das RSA-Verfahren bietet den Vorteil hoher Sicherheit, ist jedoch nur mit außerordentlich hohem Rechenaufwand durchzuführen. In einem Beitrag der Zeitschrift Computer, Nr. 9, September 1986, Seiten 21 bis 34 (Zimmermann, P.: A Proposed Standard Format for RSA Cryptosystems), wird ein Verschlüsselungsfunktionsprotokoll vorgeschlagen. Das vorgeschlagene Protokoll definiert die Datenstruktur von öffentlichen und privaten (geheimen) RSA-Schlüsseln. In diesem Zusammenhang ist vorgesehen, daß Nachrichten mit sogenannten digitalen Unterschriften unterzeichnet werden. Dabei werden eine Nachricht und die Unterschrift mit dem gemeinen Schlüssel der nachrichtenabsendenden Endstelle und gegebenenfalls mit dem öffentlichen Schlüssel der nachrichtenempfangenden Endstelle verschlüsselt.

Ausgehend von diesem Stand der Technik liegt der Erfindung die Aufgabe zugrunde, ein Verfahren zur Verschlüsselung von Nutzdaten anzugeben, das einerseits bei relativ geringem Rechenaufwand hohe Sicherheit gegen unbefugten Zugriff bietet und das andererseits den Aufwand zur sicheren Schlüsselübertragung reduziert. Diese Aufgabe wird erfindungsgemäß mit den Merkmalen des kennzeichnenden Teils des Hauptanspruchs gelöst.

Die Erfindung verknüpft also die Vorteile der symmetrischen und der asymmetrischen Verschlüsselungsverfahren. Der erforderliche Rechenaufwand läßt sich mit zum Prioritätszeitpunkt der vorliegenden Anmeldung auf dem Markt erhältlichen Bauelementen, insbesondere mit sogenannten VLSI-Chips ohne weiteres realisieren.

Die Erfindung zeichnet sich durch den weiteren Vorteil aus, daß außerhalb der Kommunikationsendstellen der beziehungsweise die Schlüssel zur Ver- und Entschlüsselung der Nutzdaten nur in verschlüsselter Form verfügbar sind und nur von berechtigten Teilnehmern mittels deren geheimen Schlüsseln benutzbar sind.

Die Erfindung wird nun anhand der Zeichnungen in einem zum Verständnis erforderlichen Umfang beschrieben. Es zeigt

Fig. 1 eine Vorrichtung zur Durchführung des Verfahrens gemäß der Erfindung;

Fig. 2 das Ablaufdiagramm des Teils des erfindungsgemäßen Verfahrens, bei dem in der ersten Kommunikationsendstelle A erster temporärer Schlüssel K_{SA1} zur weiteren Verwendung in der ersten Kommunikationsendstelle A und gleichzeitig ein zweiter temporärer Schlüssel K_{SB1} zur weiteren Verwendung in der zweiten Kommunikationsendstelle B erzeugt wird (Anspruch 1, 1. Alternative in Verbindung mit den Ansprüchen 3 und 4);

Fig. 3 das Ablaufdiagramm des Teils des erfindungsgemäßen Verfahrens, bei dem alternativ zu den in **Fig.** 2 dargestellten Verfahrensteil der erste und zweite temporäre Schlüssel K_{SA1}, K_{SB1} zeitlich versetzt, aber in gleicher Weise erzeugt werden (Anspruch 1, 2. Alternative in Verbindung mit den Ansprüchen 3 und 4);

Fig. 4 das Ablaufdiagramm des Teils des erfindungsgemäßen Verfahrens, bei dem alternativ zu den in **Fig.** 2 und 3 dargestellten Verfahrensteilen der zweite temporäre Schlüssel K_{SB1} aus dem ersten temporären Schlüssel K_{SA1} erzeugt wird (Anspruch 2 in Verbindung mit den Ansprüchen 3 und 4);

Fig. 5 das Ablaufdiagramm des Teils des erfindungsgemäßen Verfahrens, bei dem erste Nutzdaten ND_1 in der ersten Kommunikationsendstelle A verschlüsselt und die verschlüsselten Nutzdaten ND_1' an die zweite Kommunikationsendstelle B übertragen werden;

Fig. 6 das Ablaufdiagramm des Teils des erfindungsgemäßen Verfahrens, bei dem die verschlüsselten Nutzdaten ND_1' in der zweiten Kommunikationsendstelle B entschlüsselt werden.

Die in **Fig.** 1 dargestellte Vorrichtung besteht aus einer ersten und einer zweiten Kommunikationsendstelle A und B. Beide Kommunikationsendstellen A und B, die beispielsweise als sogenannte Integrated Services Digital Network (ISDN)-Endstellen ausgebildet sind, sind über ein Kommunikationssystem miteinander verbindbar, das auch unbefugten Benutzern Zugriff ermöglicht.

Dieses Kommunikationssystem besteht aus mindestens einer Verbindungsleitung und kann neben den beiden Kommunikationsendstellen A und B weitere in Fig. 1 nicht dargestellte Kommunikationsendstellen miteinander verbinden.

Jede Kommunikationsendstelle A und B besteht aus einer räumlich abgeschlossenen Verschlüsselungseinrichtung VA, VB und aus einer an die Verbindungsleitung angeschlossenen Bedienungseinrichtung TA, TB.

Die Verschlüsselungseinrichtung VA der ersten Kommunikationsendstelle A und die Verschlüsselungseinrichtung VB der zweiten Kommunikationsendstelle weisen mindestens eine erste Eingabeeinrichtung AWL_A, AWL_B zur beispielsweise manuellen Eingabe des der jeweiligen Kommunikationsendstelle A beziehungsweise B zugeordneten, aus einem geheimen Schlüssel K_{GA} beziehungsweise K_{GB} und einem öffentlichen Schlüssel K_{PA}, K_{PB} bestehenden Schlüsselpaars auf.

Die geheimen Schlüssel K_{GA} und K_{GB} können auch auf Ausweisen beziehungsweise Chipkarten abgespeichert sein. Zusätzlich können darauf auch die jeweiligen öffentlichen Schlüssel K_{PA}, K_{PB} abgespeichert sein. Die erste Eingabeeinrichtung AWL_A, beziehungsweise AWL_B ist dann als Ausweis- beziehungsweise Chipkartenlesegerät ausgebildet.

Die jeweiligen geheimen Schlüssel K_{GA} und K_{GB} können auch in besonderen Speichereinrichtungen in der jeweiligen Verschlüsselungseinrichtung VA oder VB abgespeichert sein, zum Beispiel in Form von steckbaren "Read Only Memories".

Die den beiden Kommunikationsendstellen A und B zugeordneten Schlüsselpaare K_{GA}, K_{PA}; K_{GB}, K_{PB} können aus Sicherheitsgründen jeweils eine zeitlich begrenzte Gültigkeit besitzen.

Zur Eingabe des öffentlichen Schlüssels (z. B. K_{PB}, K_{PA}) derjenigen Kommunikationsendstellen (z. B. B, A), an die Nutzdaten übertragen werden sollen, kann, wenn der betreffende öffentliche Schlüssel einem Verzeichnis entnehmbar ist, die die Nutzdaten absendende Kommunikationsendstelle (z. B. A, B) eine zweite Eingabeeinrichtung EG_A beziehungsweise EG_B aufweisen, die als alphanumerische Eingabeeinrichtung ausgebildet ist. Ist die erste Eingabeeinrichtung AWL_A beziehungsweise AWL_B alphanumerisch ausgebildet, so erübrigt sich die zweite Eingabeeinrichtung EG_A beziehungsweise EG_B. Die zweite Eingabeeinrichtung EG_A beziehungsweise EG_B erübrigt sich auch, wenn der öffentliche Schlüssel (z. B. K_{PB}, K_{PA}) an diejenige Kommunikationsendstelle (z. B. A, B) über die Verbindungsleitung übertragen wird, die die Nutzdaten verschlüsselt, um diese anschließend an die Kommunikationsendstelle (z. B. B, A) zu übertragen, der der übertragene öffentliche Schlüssel (K_{PB}, K_{PA}) zugeordnet ist.

Die öffentlichen Schlüssel K_{PA}, K_{PB} können auch über gesonderte, unten noch beschriebene Eingabeeinrichtungen E/A_A, E/A_B in den Bedieneinrichtungen TA, TB eingegeben werden und gelangen von dort, beziehungsweise von den ebenfalls in TA, TB angeordneten Speichern SP_A, SP_B über die entsprechende Schnittstellenschaltung IF_A, IF_B zur weiteren Bearbeitung in die Verschlüsselungseinrichtung VA beziehungsweise VB.

Die ersten und zweiten Eingabeeinrichtungen AWL_A, AWL_B und EG_A, EG_B sind jeweils mit einer zentralen Steuerung ZST_A, ZST_B verbunden, die wie in Fig. 1 dargestellt in den Verschlüsselungseinrichtungen VA, VB angeordnet sind und mit den Komponenten ZG_A, $E_{A,RSA}$, $D_{A,RSA}$ und IF_A beziehungsweise ZG_B, $D_{B,RSA}$, $E_{B,RSA}$ und IF_B von VA beziehungsweise VB in Verbindung steht.

Der Zufallsgenerator ZG_A in der Verschlüsselungseinrichtung VA der Kommunikationsendstelle A dient der Erzeugung der an der Kommunikation beteiligten Kommunikationsendstellen gemeinsamen temporären Schlüssel als Zufallszahlen K_{S1}, K_{S3}. Die Verschlüsselungseinrichtung VA enthält ferner eine Schnittstellenschaltung IF_A sowie ein nach einem asymmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul $E_{A,RSA}$ sowie ein nach einem asymmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{A,RSA}$. Die vier letztgenannten Komponenten ZG_A, IF_A, $E_{A,RSA}$ und $D_{A,RSA}$ werden von der zentralen Steuerung ZST_A der Kommunikationsendstelle A gesteuert. Das Entschlüsselungsmodul $D_{A,RSA}$ steht außerdem mit einem ebenfalls in der Verschlüsselungseinrichtung VA der Kommunikationsendstelle A angeordneten Verschlüsselungsmodul $E_{A,DES}$ in Verbindung. Diesem Modul werden erste Nutzdaten ND_1 zugeführt, die nach Durchführung eines symmetrischen Verschlüsselungsvorgangs ausgangsseitig als verschlüsselte Nutzdaten ND_1' über die Schnittstellenschaltung IF_A, der Bedieneinrichtung TA und die Verbindungsleitung an die zweite Kommunikationsendstelle B abgegeben werden. Die Module $E_{A,DES}$ und $D_{A,DES}$ können auch unmittelbar an die zentrale Steuerung ZST_A angeschlossen sein, so daß die Ausgangsparameter der Module $D_{A,RSA}$ und $E_{A,RSA}$ den Modulen $E_{A,DES}$ und $D_{A,DES}$ über die zentrale Steuerung ZST_A zugeführt werden.

Die zweite Kommunikationsendstelle B weist zur Durchführung des Verfahrens nach Anspruch 1 neben der Bedieneinrichtung TB in der zugeordneten Verschlüsselungseinrichtung VB die Komponenten ZST_B, AWL_B, gegebenenfalls EG_B, ein nach einem asymmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{B,RSA}$ und ein mit diesem in Verbindung stehendes, nach einem symmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{B,DES}$ auf. Dieses Entschlüsselungsmodul $D_{B,DES}$ entschlüsselt die von der ersten Kommunikationsendstelle A übertragenen verschlüsselten ersten Nutzdaten ND_1' nach einem symmetrischen Verschlüsselungsverfahren und erzeugt wieder die Originalnutzdaten ND_1.

Die zweite Kommunikationsendstelle B kann so ausgebildet sein, daß sie nicht nur von der ersten Kommunikationsendstelle A erste verschlüsselte und übertragene Nutzdaten ND_1 entschlüsselt, sondern ihrerseits zweite Nutzdaten ND_2 verschlüsselt und die zweiten verschlüsselten Nutzdaten ND_2' an die erste Kommunikationsendstelle A überträgt. Dabei kann, wie weiter unten näher erläutert wird, die Verschlüsselung der zweiten Nutzdaten ND_2 in der zweiten Kommunikationsendstelle B mittels eines von der ersten Kommunikationsendstelle A erzeugten Schlüssel K_{SB1} oder mittels eines in der zweiten Kommunikationsendstelle B erzeugten Schlüssels K_{SB2} erfolgen.

Verschlüsselt die zweite Kommunikationsendstelle B zweite Nutzdaten ND_2, so enthält ihre Verschlüsselungseinrichtung VB ein nach einem symmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul $E_{B,DES}$, während die Verschlüsselungseinrichtung VA der ersten Kommunikationseinrichtung A ein nach dem symmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{A,DES}$ zur Entschlüsselung der zweiten verschlüsselten, von der ersten Kommunikationsendstelle A übertragenen Nutzdaten

ND_2' aufweist.

Das nach dem symmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul $E_{B,DES}$ und das Entschlüsselungsmodul $D_{A,DES}$ können, wie in Fig. 1 gezeigt und unten im Zusammenhang mit dem Verfahren gemäß der Erfindung noch beschrieben wird, entweder von dem in der der Verschlüsselungseinrichtung VA oder VB erzeugten Schlüssel K_{S1} oder K_{S2} angesteuert werden.

Im letztgenannten Fall, in dem also die Verschlüsselungseinrichtung VB der zweiten Kommunikationsendstelle B einen Schlüssel K_{S2} erzeugt, weist sie einen Zufallsgenerator ZG_B zur Erzeugung von Zufallszahlen K_{S2} und ein nach einem asymmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul $E_{B,RSA}$ auf.

Fig. 1 zeigt die genannten Komponenten, ihre Verknüpfung und soweit für das Verständnis der Erfindung erforderlich ihre Ein- und Ausgangsparameter. Diejenigen Komponenten beider Kommunikationsendstellen A, B, die zusätzlich zu den zur Durchführung des erfindungsgemäßen Verfahrens nach Anspruch 1 erforderlichen Komponenten vorgesehen sein können, sind in unterbrochener Linie dargestellt.

Die Verschlüsselungseinrichtungen VA und VB können die gleichen Komponenten enthalten und baugleich sein. Damit sind die Kommunikationsendstellen A und B zur Kommunikation in den Richtungen A-B und B-A fähig, wobei sowohl A als auch B die Kommunikation einleiten kann.

Die Bedieneinrichtungen TA, TB der beiden Kommunikationsendstellen A, B sind intelligente Endgeräte und einerseits mit der beziehungsweise den zur jeweiligen anderen Kommunikationsendstelle B, A führenden Verbindungsleitung(en) und andererseits mit der Verschlüsselungseinrichtung VA beziehungsweise VB verbunden. Zur Auslösung des Verfahrens gemäß der Erfindung weist mindestens eine Kommunikationsendstelle (z. B. A) eine Einrichtung E/A_A auf. Eine entsprechende Einrichtung E/A_B kann auch die Bedieneinrichtung TB aufweisen. Die ersten beziehungsweise zweiten Nutzdaten ND_1, ND_2 können der ersten beziehungsweise zweiten Kommunikationsendstelle A, B von externen Nutzdatenquellen zugeführt werden oder in den Kommunikationsendstellen selbst, beispielsweise durch manuelle Eingabe in die Einrichtungen E/A_A, E/A_B erzeugt werden. Beide Bedieneinrichtungen TA, TB können ferner je einen Speicher SP_A, SP_B enthalten, der unter anderem zur Aufnahme temporärer Schlüssel dienen kann. Zu diesem Schlüssel gehören beispielsweise die im Zusammenhang mit dem erfindungsgemäßen Verfahren erläuterten Schlüssel K_{SA1}, K_{SA2}, K_{SB1}, K_{SB2}, in keinem Fall aber die beiden Kommunikationsendstellen A, B gemeinsamen temporären Schlüssel K_{S1}, K_{S2}, die wie ebenfalls noch erläutert wird, der Ver- beziehungsweise Entschlüsselung der ersten, zweiten und beziehungsweise dritten Nutzdaten ND_1, ND_1', ND_2, ND_2', ND_3 dienen. Diese Schlüssel K_{S1}, K_{S2} verbleiben gemäß der Erfindung nur in den Verschlüsselungseinheiten VA beziehungsweise VB, wo sie auch erzeugt werden. Sie gelangen ebensowenig wie die geheimen Schlüssel K_{GA}, K_{GB} also weder in die Bedieneinrichtungen TA beziehungsweise TB noch werden sie über die Verbindungsleitung zu der korrespondierenden Kommunikationsendstelle übertragen. In die Speicher SP_A, SP_B können außerdem die der eigenen und der korrespondierenden Kommunikationsendstelle zugeordneten öffentlichen Schlüssel K_{PA}, K_{PB} eingespeichert werden.

Die Kommunikationsendstelle A, die Nutzdaten verschlüsselt, kann auch mit einer Kommunikationsendstelle F in Verbindung stehen, die als Speichereinrichtung zur Aufnahme der verschlüsselten Nutzdaten ausgebildet ist. Eine solche Kommunikationsendstelle oder Speichereinrichtung F weist im Gegensatz zu der oben beschriebenen zweiten Kommunikationsendstelle B keine Entschlüsselungseinrichtungen auf. Ebensowenig weist eine solche Kommunikationsstelle F Komponenten auf, die der Verschlüsselung von Nutzdaten dienen. Als Beispiel für Kommunikationsstellen F seien Sprach- oder sonstige Informationen enthaltene Speicher in Kommunikationsnebenstellenanlagen genannt.

Als symmetrisches und asymmetrisches Verfahren werden bei der Erfindung insbesondere das DES- und das RSA-Verfahren verwendet. Die Module $E_{A,DES}$, $D_{A,DES}$, $E_{B,DES}$ und $D_{B,DES}$ sind dann als DES-Module und die Module $E_{A,RSA}$, $D_{A,RSA}$, $E_{B,RSA}$ und $D_{B,RSA}$ als RSA-Module ausgebildet. In den Verschlüsselungseinrichtungen VA und VB können auf dem Markt erhältliche Module verwendet werden. Als Beispiel für ein kombiniertes DES-Ver- und Entschlüsselungsmodul ($E_{A,DES}/D_{A,DES}$, $E_{B,DES}/D_{B,DES}$) sei der sogenannte AM 9518 Data Ciphering Processor des Herstellers "Advanced Micro Devices, Inc.", aus Sunnyvale, Kalifornien/Vereinigte Staaten von Amerika genannt. Als Beispiel für ein kombiniertes RSA-Ver- und Entschlüsselungsmodul ($E_{A,RSA}/D_{A,RSA}$, $E_{B,RSA}/D_{B,RSA}$) seien die Erzeugnisse "METEOR" und "METEORITE (VLSI) EXPONENTIATOR" der Herstellerfirma British TELECOM genannt.

Im folgenden wird anhand der Fig. 2 bis 6 das Verfahren, soweit es in den beiden Verschlüsselungseinrichtungen VA und VB durchgeführt wird, gemäß der Erfindung beschrieben. Dabei wird zunächst davon ausgegangen, daß die erste Kommunikationsendstelle A erste Nutzdaten ND_1' in verschlüsselter Form an die zweite Kommunikationsendstelle B überträgt, wo die verschlüsselten Nutzdaten ND_1' durch entsprechende Entschlüsselung in die Originalnutzdaten ND_1 rückgewandelt werden. Jeder Kommunikationsendstelle A, B ist ein aus einem geheimen oder privaten Schlüssel K_{GA}, K_{GB} und einem öffentlichen Schlüssel K_{PA}, K_{PB} bestehendes Schlüsselpaar zugeordnet.

Fig. 2 veranschaulicht den ersten Teil des Verfahrens gemäß der Erfindung, bei dem beispielsweise in der ersten Kommunikationsendstelle A, von der erste Nutzdaten ND_1 an die zweite Kommunikationsendstelle B übertragen werden sollen, ein erster temporärer Schlüssel K_{SA1} und ein zweiter temporärer Schlüssel K_{SB1} erzeugt werden. Der erste beziehungsweise zweite temporäre Schlüssel K_{SA1}, K_{SB1} dient wie noch erläutert wird, der Erzeugung eines ebenfalls temporären, aber beiden Kommunikationsendstellen A, B gemeinsamen Schlüssels K_{S1} zur Verschlüsselung erster Nutzdaten ND_1 in der ersten Kommunikationsendstelle A beziehungsweise zur Entschlüsselung der ersten verschlüsselten Nutzdaten ND_1' in der zweiten Kommunikationsendstelle B.

Der in der Verschlüsselungseinrichtung VA der ersten Kommunikationsendstelle A angeordnete Zufallsgenerator ZG_A generiert einen erten temporären Schlüssel K_{S1} als Zufallszahl, die beispielsweise aus 56 Bit besteht.

Im Anschluß daran wird K_{S1} mittels der zentralen Steuerung ZST_A auf beispielsweise 512 Bit expandiert, indem K_{S1} mit festen Bitfolgen, vorzugsweise jedoch mit Bitfolgen aufgefüllt wird, die aus K_{S1} abgeleitet wer-

den. Dies geschieht beispielsweise dadurch, indem an K_{S1} Bitfolgen angehängt werden, die nach einer vorgegebenen festen Regel gebildet werden. Beispielsweise werden die angehängten Bitfolgen aus K_{S1} abgeleitet. Die Expandierung beziehungsweise eine spätere Komprimierung (Fig. 5, 6) ist notwendig, wenn die beiden beim erfindungsgemäßen Verfahren benutzten Verschlüsselungsverfahren, ein asymmetrisches Verfahren, insbesondere das RSA-Verfahren, und ein symmetrisches Verfahren, insbesondere das DES-Verfahren blockorientiert, das heißt stets mit ganzzahlig Vielfachen der Blocklänge arbeiten.

Als praktikabel im Hinblick auf Sicherheit und Realisierung hat sich für das RSA-Verfahren eine Blocklänge von 512 Bit erwiesen, während das standardisierte DES-Verfahren mit einer Blocklänge von 64 Bit arbeitet.

Der vom Zufallsgenerator ZG_A erzeugte Schlüssel K_{S1} wird erfindungsgemäß nach einem asymmetrischen Verschlüsselungsverfahren, insbesondere nach dem RSA-Verschlüsselungsverfahren, verschlüsselt. Diese Verschlüsselung erfolgt mit Hilfe des Verschlüsselungsmoduls $E_{A,\,RSA}$ dem die öffentlichen Schlüssel K_{PA1} und K_{PB1} zugeführt werden. Die Verschlüsselung des expandierten ersten temporären Schlüssels K_{S1} liefert einen ersten temporären Schlüssel K_{SA1} und einen zweiten temporären Schlüssel K_{SB1}, der von der ersten Kommunikationsendstelle A mittels der zentralen Steuerung ZST_A über die Schnittstellenschaltung IF_A, die Bedieneinrichtung TA und die Verbindungsleitung an die zweite Kommunikationsendstelle B übertragen wird. Dieser an B zu übertragende Schlüssel K_{SB1}, der der späteren Entschlüsselung der ersten Nutzdaten ND_1' dient, kann unverschlüsselt oder verschlüsselt, übertragen werden. Die Verschlüsselung des zu übertragenden K_{SB1} kann beispielsweise auch nach dem erfindungsgemäßen Verfahren erfolgen. Hierzu wird beiden Kommunikationsendstellen A und B jeweils ein Schlüssel K_{SA0}, K_{SB0} fest zugeordnet, der von der jeweiligen Verschlüsselungseinrichtung VA beziehungsweise VB zu einem beiden Endstellen A und B gemeinsamen Schlüssel K_{S0} verarbeitet wird. K_{SA0}, K_{SB0} werden nur für die Ver- und Entschlüsselung des zu übertragenden K_{SB1} verwendet. Damit lassen sich Schlüsselhierarchien realisieren, bei denen in den Endstellen nur individuelle, übergeordnete Schlüssel (K_{SA0}, K_{SB0}), nicht jedoch identische Schlüssel (K_{S0}) wie im Stand der Technik abgespeichert werden.

Fig. 2 zeigt die gleichzeitige Erzeugung der beiden Schlüssel K_{SA1} und K_{SB1}. Beide Schlüssel können, wie in Fig. 3 dargestellt, jedoch auch zeitlich versetzt, aber in sonst gleicher Weise erzeugt werden. Dies geschieht in den folgenden Schritten: Erzeugung von K_{S1}, Expandierung, Verschlüsselung des expandierten K_{S1} mit dem öffentlichen Schlüssel K_{PA}, damit Bildung des ersten temporären Schlüssels K_{SA1} (Fig. 3); Verschlüsselung des expandierten K_{S1} mit dem öffentlichen Schlüssel K_{PB}, damit Bildung des zweiten temporären Schlüssels K_{SB1}.

Die separate Bildung des ersten temporären Schlüssels K_{SA1} ermöglicht eine Bildung des zweiten temporären Schlüssels K_{SB1} nach Fig. 4. Die zentrale Steuerung ZST_A führt dem nach einem asymmetrischen Verfahren, insbesondere nach dem RSA-Verfahren arbeitenden Entschlüsselungsmodul $D_{A,\,RSA}$ den ersten temporären Schlüssel K_{SA1} sowie den geheimen oder privaten Schlüssel K_{GA} zu. $D_{A,\,RSA}$ liefert K_{S1}, den beiden Kommunikationsstellen A, B gemeinsamen Schlüssel, der aber aus Sicherheitsgründen die Verschlüsselungseinrichtung VA nicht verläßt. Vom Ausgang des Entschlüsselungsmoduls $D_{A,\,RSA}$ wird $K_{S\,1}$ über die zentrale Steuerung ZST_A zusammen mit dem öffentlichen Schlüssel K_{PB} an das nach einem asymmetrischen Verfahren, insbesondere nach dem RSA-Verfahren arbeitende Verschlüsselungsmodul $E_{A,\,RSA}$ geschaltet. Das K_{SB1} erzeugt. K_{SB1} wird wie Fig. 1 zeigt mittels der zentralen Steuerung ZST_A über die Schnittstellenschaltung IF_A, die Bedieneinrichtungen TA und TB der Verschlüsselungseinrichtung VB zugeführt.

Fig. 5 veranschaulicht den Teil des Verfahrens gemäß der Erfindung, in dem die Verschlüsselung der Nutzdaten ND_1 in VA erfolgt. Der erste temporäre Schlüssel K_{SA1}, der im ersten Verfahrensabschnitt in der ersten Kommunikationsendstelle A entsprechend Fig. 2 oder Fig. 3 erzeugt wurde und in dem in der Bedieneinrichtung TA angeordneten Speicher SP_A zwischengespeichert werden kann, wird mit dem beispielsweise über die erste Eingabeeinrichtung AWL_A einzugebenden privaten (RSA-)Schlüssel K_{GA} entschlüsselt und dabei wird ein beiden Kommunikationsendstellen A und B gemeinsamer erster temporärer Schlüssel K_{S1} mittels des Entschlüsselungsmoduls $D_{A,\,RSA}$ gebildet. Der auf diese Weise gebildete Schlüssel dient der Verschlüsselung der ersten Nutzdaten ND_1 nach einem symmetrischen Verschlüsselungsverfahren, insbesondere nach dem DES-Verschlüsselungsverfahren. Vor der DES-Verschlüsselung wird der erste temporäre Schlüssel auf die DES-Schlüssellänge von 56 Bit komprimiert. Die ersten Nutzdaten ND_1, die der Kommunikationsendstelle A von einer externen Datenquelle zugeführt oder beispielsweise mittels der in der Bedieneinrichtung TA angeordneten Eingabeeinrichtung E/A_A erzeugt werden können, werden in der Verschlüsselungseinrichtung VA über die Schnittstellenschaltung IF_A mittels der zentralen Steuerung ZST_A an den Eingang des Verschlüsselungsmoduls $E_{A,\,DES}$ durchgeschaltet. Das Ergebnis der DES-Verschlüsselung der Daten ND_1 mit dem komprimierten ersten temporären Schlüssel K_{S1} liefert verschlüsselte Daten ND_1', die über die Schnittstellenschaltung IF_A und die Bedieneinrichtung TA an die zweite Kommunikationsendstelle B zur dortigen Entschlüsselung übertragen werden.

Über die Verbindungsleitung werden zwischen den Kommunikationsendstellen A und B also der zweite temporäre (RSA-)Schlüssel K_{SB1} und die (DES-) verschlüsselten Nutzdaten ND_1' übertragen. Der zweite temporäre (RSA-)Schlüssel K_{SB1} ist nur durch den geheimen, der Kommunikationsendstelle B zugeordneten (RSA-)Schlüssel K_{GB} entschlüsselbar. Die (DES-) verschlüsselten Nutzdaten ND_1' sind nur mit dem beiden Kommunikationsendstellen A, B gemeinsamen (DES-)Schlüssel K_{S1} entschlüsselbar, der in der Verschlüsselungseinheit VB aus dem zweiten temporären (RSA-)Schlüssel K_{S1} mit Hilfe des geheimen Schlüssels K_{GB} erzeugt wird.

Fig. 6 veranschaulicht den abschließenden Abschnitt des Verfahrens gemäß der Erfindung, bei dem die von A übertragenen ersten verschlüsselten Nutzdaten ND_1' in VB entschlüsselt werden. Der von der ersten Kommunikationsendstelle A übertragene zweite temporäre Schlüssel K_{SB1}, der im Speicher SP_B der Bedieneinrichtung TB zwischenspeicherbar ist, wird mit Hilfe der zentralen Steuerung ZST_B über die Schnittstellenschaltung IF_B dem Entschlüsselungsmodul $D_{B,\,RSA}$ zugeführt und mit dem, beispielsweise über die erste Eingabeeinrichtung AWL_B einzugebenden privaten (RSA-)Schlüssel K_{GB} entschlüsselt. Das Ergebnis dieses Entschlüsselungsvorgangs ist der beiden Kommunikationsendstel-

len A und B gemeinsame erste temporäre Schlüssel K_{S1}. Dieser Schlüssel dient der Entschlüsselung der verschlüsselten ersten Nutzdaten ND_1'. Er wird vom Ausgang des (RSA-)Entschlüsselungsmoduls $D_{B,RSA}$ an den Steuereingang des Entschlüsselungsmoduls $D_{B,DES}$ durchgeschaltet. Die Entschlüsselung erfolgt nach einem symmetrischen, insbesondere nach dem DES-Verfahren. Vor der DES-Entschlüsselung wird der erste temporäre Schlüssel K_{S1} auf die DES-Schlüssellänge von 56 Bit komprimiert. Die verschlüsselten Nutzdaten ND_1' gelangen über die Bedieneinrichtung TB und die Schnittstellenschaltung IF_B an das Entschlüsselungsmodul $D_{B,DES}$. Die entschlüsselten Nutzdaten ND_1 gelangen über die Schnittstellenschaltung IF_B an die Bedieneinrichtung TB zurück, wo sie ausgewertet oder von wo sie an eine externe Nutzdatensenke weitergegeben werden können.

Verschlüsselte Nutzdaten lassen sich auch von der zweiten zur ersten Kommunikationsendstelle, also von B nach A, übertragen.

Dabei sind zwei Fälle zu unterscheiden:

1. Die von B nach A zu übertragenden zweiten Nutzdaten ND_2 werden in der Verschlüsselungseinrichtung VB mit dem ersten temporären Schlüssel K_{S1} verschlüsselt, der sowohl in VB als auch in VA wie beschrieben aus K_{SB1} und K_{SA1} zu bilden ist, und
2. Die von B nach A zu übertragenden zweiten Nutzdaten ND_2 werden in der Verschlüsselungseinrichtung VB mit einem zweiten temporären Schlüssel K_{S2} verschlüsselt.

Im ersten Fall, bei dem zweite Nutzdaten ND_2 mit dem ersten temporären Schlüssel K_{S1} verschlüsselt werden, wird dieser aus K_{SB1} und K_{GB} (analog **Fig. 5**) vom Ausgang des (RSA-)Entschlüsselungsmodul $D_{B,RSA}$ an den Eingang des (DES-)Verschlüsselungsmoduls $E_{B,DES}$ durchgeschaltet. Die zweiten verschlüsselten Nutzdaten ND_2' gelangen vom Ausgang des Verschlüsselungsmoduls $E_{B,DES}$ über die Schnittstellenschaltung IF_B, die Bedieneinrichtung TB, die Verbindungsleitung, die Bedieneinrichtung TA, und die Schnittstellenschaltung IF_A an den Eingang des (DES-)Entschlüsselungsmoduls $D_{A,DES}$, das von dem ersten temporären K_{S1} gesteuert wird. K_{S1} wird in VA aus K_{SA1} und K_{GA} (analog **Fig. 5**) gebildet.

Im zweiten Fall, bei dem zweite Nutzdaten ND_2 mit einem zweiten temporären Schlüssel K_{S2} in VB verschlüsselt werden, ist dieser dort zunächst zu bilden. Die Bildung dieses Schlüssels K_{S2}, der Ver- und Entschlüsselung der zweiten Nutzdaten ND_2 beziehungsweise ND_2' in der zweiten und ersten Kommunikationsendstelle B, A erfolgt dabei analog zu den anhand **Fig. 2—6** beschriebenen Verfahrensschritte:

Der in der Verschlüsselungseinrichtung VB angeordnete Zufallsgenerator ZG_B erzeugt einen zweiten beiden Kommunikationsendstellen B, A gemeinsamen temporären Schlüssel K_{S2} als eine zweite Zufallszahl, die der zentralen Steuerung ZST_B zugeführt und gegebenenfalls nach einer entsprechenden Expandierung von 56 Bit auf 512 Bit dem (RSA-)Verschlüsselungsmodul $E_{B,RSA}$ zusammen mit dem öffentlichen Schlüssel K_{PB} zugeführt wird. Dem Verschlüsselungsmodul $E_{B,RSA}$ wird außerdem der öffentliche Schlüssel K_{PA} zugeführt. Es erzeugt gleichzeitig oder zeitlich versetzt analog zu den anhand der **Fig. 2** beziehungsweise **Fig. 3** und **4** beschriebenen Verfahrensschritte einen weiteren temporären Schlüssel K_{SB2} und einen weiteren zweiten temporären Schlüssel K_{SA2}, der an die erste Kommunikationsendstelle A übertragen wird.

Das Entschlüsselungsmodul $D_{B,RSA}$ entschlüsselt mit dem der zweiten Kommunikationsendstelle B zugeordneten geheimen Schlüssel K_{GB} den weiteren ersten Schlüssel K_{SB2} und bildet damit den beiden Kommunikationsendstellen B, A gemeinsamen zweiten temporären Schlüssel K_{S2}. Der Schlüssel K_{S2} wird dem Steuereingang des Verschlüsselungsmoduls $E_{B,DES}$ zugeführt, daß die ihm ebenfalls zugeführten zweiten Nutzdaten ND_2 verschlüsselt. Die verschlüsselten zweiten Nutzdaten ND_2' werden an die erste Kommunikationsendstelle A übertragen. Dort wird zunächst der von A übertragene (RSA-)Schlüssel K_{SA2} durch das Entschlüsselungsmodul $D_{A,RSA}$ entschlüsselt. Der dabei entstehende zweite temporäre Schlüssel K_{S2} wird dem Steuereingang des Entschlüsselungsmoduls $D_{A,DES}$ zugeführt, das die zweiten Nutzdaten ND_2' entschlüsselt. Die zweiten entschlüsselten Nutzdaten ND_2 werden über die Schnittstellenschaltung IF_A der Bedieneinrichtung TA zugeführt, wo sie ausgewertet oder von wo sie an eine externe Nutzdatensenke weitergegeben werden können.

Bei dem hier beschriebenen Verfahren erfolgt die Verschlüsselung der in der Richtung A-B zu übertragenden ersten Nutzdaten ND_1 nach dem ersten temporären Schlüssel K_{S1} und zur Erhöhung der Sicherheit erfolgt die Verschlüsselung der in der Richtung B-A zu übertragenden zweiten Nutzdaten nach dem zweiten temporären Schlüssel K_{S2}.

Die zweite Kommunikationsendstelle B kann ebenso, wie das für die Schlüsselbildung in der ersten Kommunikationsendstelle A anhand der **Fig. 2, 3** und **4** erläutert wurde, den weiteren zweiten Schlüssel K_{SA2} nicht nur durch Verschlüsselung des vom Zufallsgenerator ZG_B erzeugten, A und B gemeinsamen zweiten temporären Schlüssels K_{S2} mit dem öffentlichen Schlüssel K_{PA} von A bilden, sondern auch durch Entschlüsselung des weiteren ersten temporären Schlüssels K_{SB2} mit dem eigenen geheimen Schlüssel K_{GB} und durch Verschlüsselung des so gebildeten, den beiden Kommunikationsendstellen B, A gemeinsamen zweiten temporären Schlüssel K_{S2} mit dem öffentlichen Schlüssel K_{PA} von A.

Die zweite Kommunikationsendstelle B erzeugt den weiteren ersten und den weiteren zweiten temporären Schlüssel K_{SB2}, K_{SA2} insbesondere nach dem RSA-Verfahren und bildet nach diesem Verfahren den beiden Kommunikationsendstellen A, B gemeinsamen zweiten temporären Schlüssel K_{S2}. Die erste Kommunikationsendstelle A entschlüsselt dann den weiteren zweiten temporären Schlüssel K_{SA2} ebenfalls nach diesem Verfahren.

Die zweiten unverschlüsselten beziehungsweise verschlüsselten Nutzdaten ND_2, ND_2' werden insbesondere nach dem DES-Verfahren ver- beziehungsweise entschlüsselt.

Wie oben im Zusammenhang mit **Fig. 1** erläutert wurde, kann die Kommunikationsendstelle A, die Nutzdaten verschlüsselt, auch mit einer Kommunikationsendstelle F in Verbindung stehen, die als Speichereinrichtung zur Aufnahme der verschlüsselten Nutzdaten ausgebildet ist. Im Gegensatz zu der beschriebenen Kommunikationsendstelle B weist eine Kommunikationsendstelle F keine Entschlüsselungseinrichtungen auf. Der Kommunikationsendstelle A ist wiederum ein aus einem geheimen und einem öffentlichen Schlüssel bestehendes Schlüsselpaar K_{GA}, K_{PA} zugeordnet. Sie erzeugt mit

ihrem Zufallsgenerator ZG_A eine dritte Zufallszahl K_{S3} und, analog wie oben anhand **Fig. 3** beschrieben, aus dieser dritten Zufallszahl K_{S3}, gegebenenfalls nach einer Expandierung, mit ihrem öffentlichen Schlüssel K_{PA} nach einem asymmetrischen Verschlüsselungsverfahren, insbesondere nach dem RSA-Verfahren, einen dritten temporären Schlüssel K_{SA3}. Dieser Schlüssel K_{SA3} wird anschließend mit dem geheimen Schlüssel K_{GA} entschlüsselt. Das Ergebnis des Entschlüsselungsvorgangs ist ein dritter temporärer Haupt-Schlüssel K_{S3}. K_{S3} wird also wie K_{S1} und K_{S2} gebildet.

Dritte Nutzdaten ND_3 werden nach einem symmetrischen Verschlüsselungsverfahren, insbesondere nach dem DES-Verfahren, verschlüsselt und die dritten verschlüsselten Nutzdaten ND_3' werden an die Speichereinrichtung F übertragen und in verschlüsselter Form abgespeichert. Die Kommunikationsendstelle A kann die verschlüsselten Daten ND_3' jederzeit abrufen oder entschlüsseln. Der dritte temporäre Schlüssel K_{SA3} ist in der Zeit zwischen Ver- und Entschlüsselung der Nutzdaten ND_3 beziehungsweise ND_3', in der diese in F abgespeichert sind, ebenfalls abzuspeichern, beispielsweise in dem in der Bedieneinrichtung TA angeordneten Speicher SP_A. Die Entschlüsselung erfolgt mit dem temporären Haupt-Schlüssel K_{S3}, den A mit dem in Zwischenzeit abgespeicherten dritten temporären Schlüssel K_{SA3} und mit dem geheimen Schlüssel K_{GA} neu bildet.

Aus Sicherheitsgründen werden Kommunikationsendstellen in zeitlichen Abständen neue, jeweils aus einem geheimen und einem öffentlichen Schlüssel bestehende Schlüsselpaare zugeordnet. Dabei tritt der Fall auf, daß einer Kommunikationsendstelle ein neues Schlüsselpaar zu einem Zeitpunkt zugeordnet wird, zu dem für sie nach dem alten Schlüsselpaar verschlüsselte Nutzdaten abgespeichert sind. Die betreffende Kommunikationsendstelle hat in einem solchen Fall den abgespeicherten ursprünglich geltenden $K_{SA3(alt)}$ entsprechend den anhand von **Fig. 4** dargestellten Verfahrensschritten mit dem ursprünglich geheimen Schlüssel $K_{GA(alt)}$ zu entschlüsseln. Der Entschlüsselungsvorgang liefert den stets gleichen Hauptschlüssel K_{S3}. Dieser wird mit dem neuen öffentlichen Schlüssel $K_{PA(neu)}$ verschlüsselt. Es entsteht $K_{SA3(neu)}$, aus dem später zu einer Entschlüsselung der verschlüsselten Nutzdaten ND_3' wieder K_{S3} gebildet werden kann. Eine Entschlüsselung der verschlüsselten Nutzdaten ND_3', die zum Zeitpunkt der Schlüsselpaaränderung abgespeichert sind, und ihre anschließende Verschlüsselung ist wegen der Schlüsselpaaränderung nicht erforderlich.

Eine Kommunikationsendstelle A kann nicht nur an die zweite Kommunikationsendstelle B erste verschlüsselte Nutzdaten ND_1' übertragen, sondern auch an weitere Kommunikationsendstellen C, D, ... N. Sie erzeugt dann zweite temporäre Schlüssel K_{SB1}, K_{SC1}, K_{SD1}, ... K_{SN1} entsprechend der anhand **Fig. 4** beschriebenen Verfahrensschritte, indem der erste temporäre Schlüssel K_{SA1} mit K_{GA} entschlüsselt wird. Der sich ergebende, allen Kommunikationsendstellen A, B, C, D, ... N gemeinsame erste temporäre Schlüssel K_{S1} wird dann in der Verschlüsselungseinrichtung VA mit den öffentlichen Schlüsseln K_{PB}, K_{PC}, K_{PD}, ... K_{PN} der Kommunikationsendstellen B, C, D, ... N verschlüsselt. Dieser Verschlüsselungsvorgang liefert K_{SB1}, K_{SC1}, K_{SD1}, ... K_{SN1}. Anschließend überträgt die erste Kommunikationsendstelle A den jeweiligen zweiten temporären Schlüssel K_{SB1}, K_{SC1}, ... K_{SN1} an die zugehörige Kommunikationsendstelle B, C, D, ... N.

Patentansprüche

1. Verfahren zur Verschlüsselung von Nutzdaten, die zwischen einer ersten und einer zweiten Kommunikationsendstelle (A, B) übertragen werden, denen jeweils ein aus einem geheimen und einem öffentlichen Schlüssel (K_{GA}, K_{GB}, K_{PA}, K_{PB}) bestehendes Schlüsselpaar zugeordnet ist, **dadurch gekennzeichnet**, daß die erste Kommunikationsendstelle (A) einen ersten beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S1}) als Zufallszahl (K_{S1}) erzeugt und aus diesen temporären Schlüssel (K_{S1}) nach einem asymetrischen Verschlüsselungsverfahren mit ihrem öffentlichen Schlüssel (K_{PA}) einen ersten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA1}) und mit dem öffentlichen Schlüssel (K_{PB}) der zweiten Kommunikationsendstelle (B) einen zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB1}) gleichzeitig oder zeitlich versetzt erzeugt und diesen an die zweite Kommunikationsendstelle (B) überträgt, daß die erste Kommunikationsendstelle (A) mit dem eigenen geheimen Schlüssel (K_{GA}) den ersten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA1}) entschlüsselt, damit den ersten beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S1}) bildet, mit dem sie erste Nutzdaten (ND_1) nach einem symmetrischen Verschlüsselungsverfahren verschlüsselt, und daß sie die verschlüsselten ersten Nutzdaten (ND_1') an die zweite Kommunikationsendstelle (B) überträgt, daß die zweite Kommunikationsendstelle (B) den zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB1}) mit dem eigenen geheimen Schlüssel (K_{GB}) entschlüsselt und damit den beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S1}) bildet, mit dem sie anschließend die von der ersten Kommunikationsendstelle (A) übertragenen, verschlüsselten ersten Nutzdaten (ND_1') entschlüsselt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die erste Kommunikationsendstelle (A) den ersten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA1}) mit dem eigenen geheimen Schlüssel (K_{GA}) entschlüsselt, damit den ersten beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S1}) bildet, diesen Schlüssel (K_{S1}) mit dem öffentlichen Schlüssel (K_{PB}) der zweiten Kommunikationsendstelle (B) verschlüsselt und damit den zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB1}) bildet.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die erste Kommunikationsendstelle (A) den ersten und zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA1}, K_{SB1}) nach dem asymmetrischen RSA-Verschlüsselungsverfahren erzeugt und nach diesem Verschlüsselungsverfahren den ersten beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S1}) bildet und daß die zweite Kommunikationsendstelle (B) den zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB1}) ebenfalls nach diesem Verschlüsselungsverfahren entschlüsselt.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die ersten

unverschlüsselten beziehungsweise verschlüsselten Nutzdaten (ND_1, ND_1') nach dem symmetrischen DES-Verschlüsselungsverfahren ver- beziehungsweise entschlüsselt werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die zweite Kommunikationsendstelle (B) zur ersten Kommunikationsendstelle (A) zu übertragende zweite Nutzdaten (ND_2) ebenfalls mit dem ersten den beiden Kommunikationsendstellen (A, B) gemeinsamen ersten temporären Schlüssel (K_{S1}) verschlüsselt, mit dem die erste Kommunikationsendstelle (A) anschließend die von der zweiten Kommunikationsendstelle (B) übertragenen, verschlüsselten zweiten Nutzdaten (ND_2') entschlüsselt.

6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die zweite Kommunikationsendstelle (B) einen zweiten beiden Kommunikationsendstellen (B, A) gemeinsamen temporären Schlüssel (K_{S2}) als Zufallszahl (K_{S2}) erzeugt und aus diesem temporären Schlüssel (K_{S2}) nach einem asymmetrischen Verschlüsselungsverfahren mit ihrem öffentlichen Schlüssel (K_{PB}) einen weiteren ersten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB2}) und mit dem öffentlichen Schlüssel (K_{PA}) der ersten Kommunikationsendstelle (A) einen weiteren zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA2}) gleichzeitig oder zeitlich versetzt erzeugt und diesen an die erste Kommunikationsendstelle (A) überträgt, daß die zweite Kommunikationsendstelle (B) mit dem eigenen geheimen Schlüssel (K_{GB}) den weiteren ersten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB2}) entschlüsselt und damit den zweiten beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S2}) bildet, mit dem sie anschließend zweite Nutzdaten (ND_2) nach einem symmetrischen Verschlüsselungsverfahren verschlüsselt, und daß sie die verschlüsselten zweiten Nutzdaten (ND_2') an die erste Kommunikationsendstelle (A) überträgt, daß die erste Kommunikationsendstelle (A) den weiteren zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA2}) mit dem eigenen geheimen Schlüssel (K_{GA}) entschlüsselt und damit den zweiten beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S2}) bildet, mit dem sie anschließend die von der zweiten Kommunikationsendstelle (B) übertragenen, verschlüsselten zweiten Nutzdaten (ND_2') entschlüsselt.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß die zweite Kommunikationsendstelle (B) den weiteren ersten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB2}) mit dem eigenen geheimen Schlüssel (K_{GB}) entschlüsselt, damit den zweiten beiden Kommunikationsendstellen (A, B) gemeinsamen zweiten temporären Schlüssel (K_{S2}) bildet, diesen Schlüssel (K_{S2}) mit dem öffentlichen Schlüssel (K_{PA}) der ersten Kommunikationsendstelle (A) verschlüsselt und damit den weiteren zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA2}) bildet.

8. Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß die zweite Kommunikationsendstelle (B) den weiteren ersten und den weiteren zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SB2}, K_{SA2}) nach dem asymmetrischen RSA-Verschlüsselungsverfahren erzeugt und nach diesem Verschlüsselungsverfahren den zweiten beiden Kommunikationsendstellen (A, B) gemeinsamen temporären Schlüssel (K_{S2}) bildet und daß die erste Kommunikationsendstelle (A) den weiteren zweiten kommunikationsendstellenindividuellen temporären Schlüssel (K_{SA2}) ebenfalls nach diesem Verschlüsselungsverfahren entschlüsselt.

9. Verfahren nach einem der Ansprüche 5 bis 8, dadurch gekennzeichnet, daß die zweiten unverschlüsselten beziehungsweise verschlüsselten Nutzdaten (ND_2, ND_2') nach dem symmetrischen DES-Verschlüsselungsverfahren ver- beziehungsweise entschlüsselt werden.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß beiden Kommunikationsendstellen (A, B) ein individueller Schlüssel (K_{SA0}, K_{SB0}) zugeordnet wird, der in der jeweiligen Kommunikationsendstelle (A, B) mit dem eigenen geheimen Schlüssel (K_{GA}, K_{GB}) nach einem asymmetrischen Verschlüsselungsverfahren entschlüsselt wird, womit ein beiden Kommunikationsendstellen (A, B) gemeinsamer Schlüssel (K_{S0}) gebildet wird, mit dem der zweite kommunikationsendstellenindividuelle temporäre Schlüssel (K_{SB1}) beziehungsweise der weitere zweite temporäre Schlüssel vor seiner Übertragung verschlüsselt beziehungsweise nach seiner Übertragung entschlüsselt wird.

11. Verfahren zur Verschlüsselung von Nutzdaten, die zwischen einer Kommunikationsendstelle (A) und einer Speichereinrichtung (F) zur Speicherung verschlüsselter Nutzdaten übertragen werden, bei dem der Kommunikationsendstelle (A) ein aus einem geheimen und einem öffentlichen Schlüssel (K_{GA}, K_{PA}) bestehendes Schlüsselpaar zugeordnet ist, dadurch gekennzeichnet, daß die Kommunikationsendstelle (A) eine Zufallszahl erzeugt und aus dieser mit ihrem öffentlichen Schlüssel (K_{PA}) nach einem asymmetrischen Verschlüsselungsverfahren einen dritten temporären Schlüssel (K_{SA3}) erzeugt, den sie mit ihrem geheimen Schlüssel (K_{GA}) entschlüsselt und damit einen weiteren Schlüssel (K_{S3}) bildet, mit dem sie dritte Nutzdaten (ND_3) nach einem symmetrischen Verschlüsselungsverfahren verschlüsselt, daß sie die dritten verschlüsselten Nutzdaten (ND_3') an die Speichereinrichtung (F) überträgt und dort abspeichert, daß sie zur Entschlüsselung der dritten abgespeicherten Nutzdaten (ND_3') diese aus der Speichereinrichtung (F) abruft und mit einem Schlüssel entschlüsselt, den sie mit dem dritten temporären Schlüssel (K_{S3}) und mit dem geheimen Schlüssel (K_{GA}) neu bildet.

12. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 1, bestehend aus einer ersten und einer mit dieser über mindestens eine Verbindungsleitung verbindbaren zweiten Kommunikationsendstelle (A, B), dadurch gekennzeichnet, daß jede Kommunikationsendstelle (A, B) aus einer räumlich abgeschlossenen Verschlüsselungseinrichtung (VA, VB) und aus einer an die Verbindungsleitung angeschlossenen Bedieneinrichtung (TA, TB) besteht, daß die Verschlüsselungseinrichtung (VA) der ersten Kommunikationsendstelle (A) und die Verschlüsselungseinrichtung (VB) der zweiten Kommunikationsendstelle (B) mindestens eine erste Eingabeeinrichtung (AWL_A, AWL_B) zur Eingabe des

der jeweiligen Kommunikationsendstelle (A, B) zugeordneten, aus einem geheimen Schlüssel (K_{GA}, K_{GB}) und einem öffentlichen Schlüssel (K_{PA}, K_{PB}) bestehenden Schlüsselpaars und eine Schnittstellenschaltung (IF_A, IF_B) aufweist, daß die Verschlüsselungseinrichtung (VA) der ersten Kommunikationsendstelle (A) ein nach dem asymmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul ($E_{A, RSA}$) und Entschlüsselungsmodul ($D_{A, RSA}$), einen Zufallsgenerator (ZG_A) und eine zentrale Steuerung (ZST_A) aufweist, die mit den vorgenannten Komponenten (AWL_A, $E_{A, RSA}$, $D_{A, RSA}$, ZG_A, IF_A) der Verschlüsselungseinrichtung (VA) der ersten Kommunikationsendstelle (A) in Verbindung steht, daß die Verschlüsselungseinrichtung (VA) der ersten Kommunikationsendstelle (A) ein nach dem symmetrischen Verschlüsselungsverfahren arbeitendes, mit dem Entschlüsselungsmodul ($D_{A, RSA}$) und mit der Schnittstellenschaltung (IF_A) in Verbindung stehendes Verschlüsselungsmodul ($E_{A, DES}$) enthält, daß die Schnittstellenschaltung (IF_A) der ersten Kommunikationsendstelle (A) ferner mit deren Bedieneinrichtung (TA) in Verbindung steht, die verschlüsselte Nutzdaten an die Verbindungsleitung abgibt beziehungsweise von dieser aufnehmen kann und die eine Einrichtung (E/A_A) zur Auslösung des Verfahrens aufweist, daß die Bedieneinrichtung (TB) der zweiten Kommunikationsendstelle (B) in analoger Weise wie die Bedieneinrichtung (TA) der ersten Kommunikationsendstelle (A) ausgebildet ist und eine Einrichtung (E/A_B) aufweist und daß die Verschlüsselungseinrichtung (VB) der zweiten Kommunikationsendstelle (B) eine zentrale Steuerung (ZST_B), ein mit ihr verbundenes, nach dem asymmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul ($D_{B, RSA}$) und ein mit diesem verbundenes, nach dem symmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul ($D_{B, DES}$), das ebenso wie die zentrale Steuerung (ZST_B) der zweiten Komunikationsendstelle (B) mit der zugehörigen Schnittstellenschaltung (IF_B) in Verbindung steht.

13. Vorrichtung nach Anspruch 12, dadurch gekennzeichnet, daß die Verschlüsselungseinrichtung (VB) der zweiten Kommunikationsendstelle (B) zusätzlich ein mit deren zentraler Steuerung (ZST_B) verbundenes, nach dem asymmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul ($E_{B, RSA}$), einen ebenfalls mit dieser zentralen Steuerung (ZST_B) verbundenen Zufallsgenerator (ZG_B) und ein nach dem asymmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul ($E_{B, DES}$) aufweist, das einerseits mit der Verschlüsselungseinrichtung (VB) der zweiten Kommunikationsendstelle (B) angeordneten Entschlüsselungsmodul ($D_{B, RSA}$) und andererseits mit der zugehörigen Schnittstellenschaltung (IF_B) in Verbindung steht.

14. Vorrichtung nach Anspruch 12 oder 13, dadurch gekennzeichnet, daß die erste und/oder zweite Kommunikationsendstelle (A, B) in ihrer jeweiligen Verschlüsselungseinrichtung (VA, VB) eine zweite Eingabeeinrichtung (EG_A, EG_B) zur Eingabe des öffentlichen Schlüssels (K_{PB}, K_{PA}) der jeweils anderen Kommunikationsendstelle (B, A) aufweist.

15. Vorrichtung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, daß die nach dem asymmetrischen Verschlüsselungsverfahren arbeitenden Verschlüsselungsmodule ($E_{A, RSA}$, $E_{B, RSA}$) der ersten und zweiten Kommunikationsendstelle (A, B) als RSA-Entschlüsselungsmodule und die nach dem asymmetrischen Verschlüsselungsverfahren arbeitenden Entschlüsselungsmodule ($D_{A, RSA}$, $D_{B, RSA}$) der ersten und zweiten Kommunikationsendstelle (A, B) als RSA-Entschlüsselungsmodule ausgebildet sind.

16. Vorrichtung nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, daß die nach dem symmetrischen Verschlüsselungsverfahren arbeitenden Verschlüsselungsmodule ($E_{A, DES}$, $E_{B, DES}$) der ersten und zweiten Kommunikationsendstelle (A, B) als DES-Verschlüsselungsmodule und die nach dem symmetrischen Verschlüsselungsverfahren arbeitenden Entschlüsselungsmodule ($D_{A, DES}$, $D_{B, DES}$) der ersten und zweiten Kommunikationsendstelle (A, B) als DES-Entschlüsselungsmodule ausgebildet sind.

17. Vorrichtung nach einem der Ansprüche 12—16, dadurch gekennzeichnet, daß die Bedieneinrichtung (TA, TB) der ersten und/oder zweiten Kommunikationsendstelle (A, B) einen Speicher (SP_A, SP_B) zur Aufnahme temporärer nicht geheimer Schlüssel (K_{SA0}, K_{SA1}, K_{SA2}, K_{SB0}, K_{SB1}, K_{SB2}; K_{PA}, K_{PB}) aufweist.

Hierzu 4 Seite(n) Zeichnungen

— Leerseite —

...mmer: DE 38 31 797 C2
...Cl.[5]: H 04 L 9/00
Veröffentlichungstag: 22. Oktober 1992

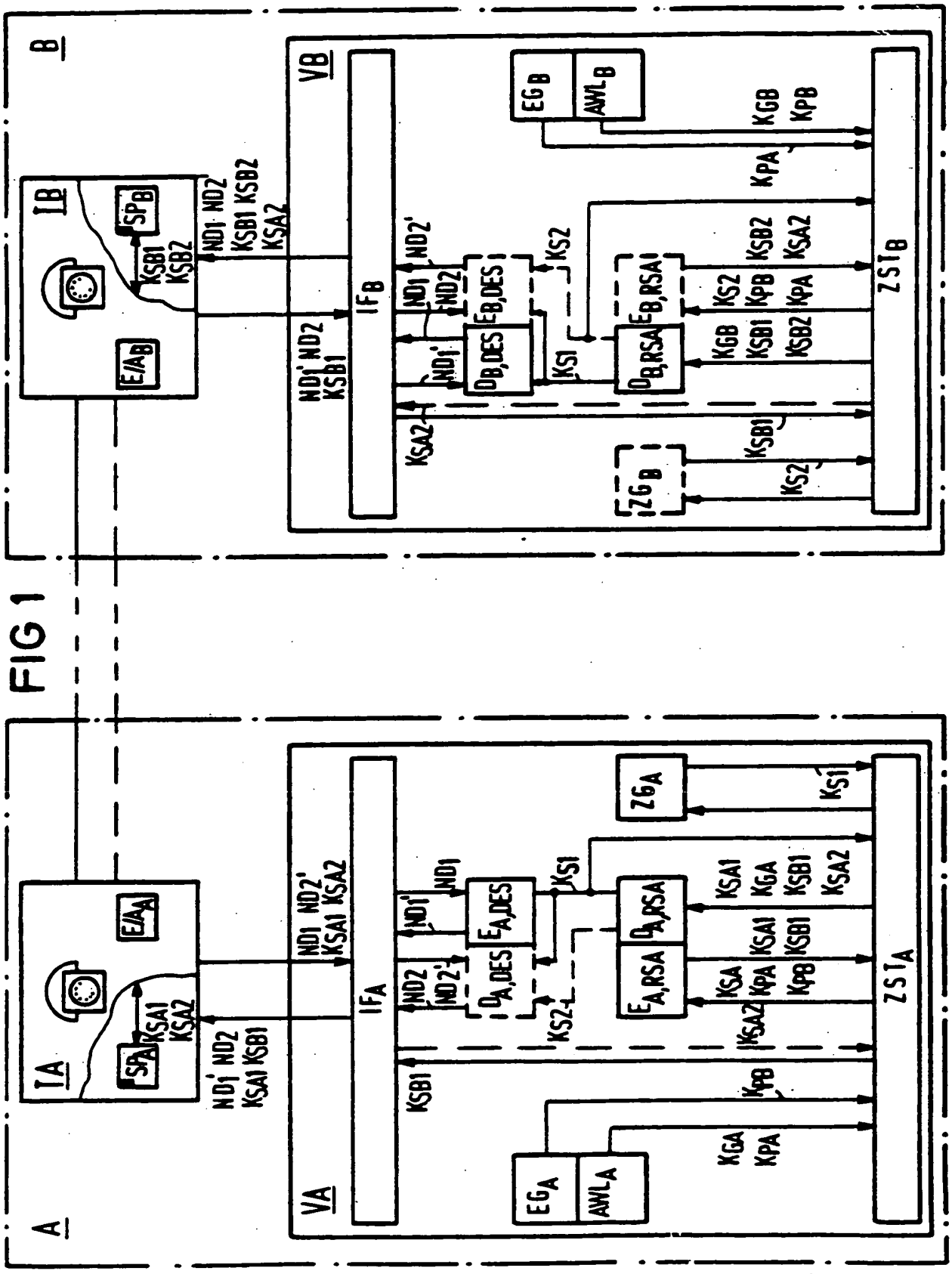


FIG 1

Nummer: DE 38 31 797 C2
Int. Cl.[5]: H 04 L 9/00
Veröffentlichungstag: 22. Oktober 1992

FIG 2

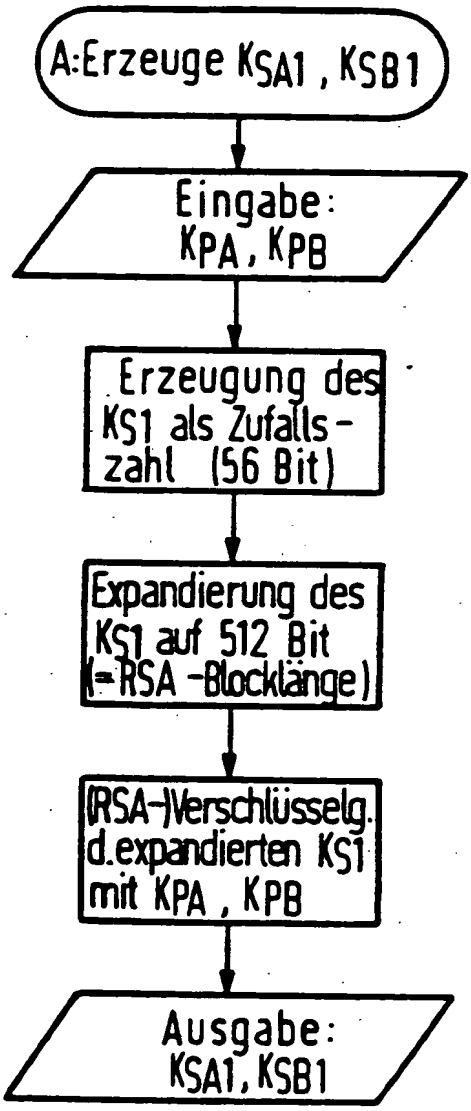
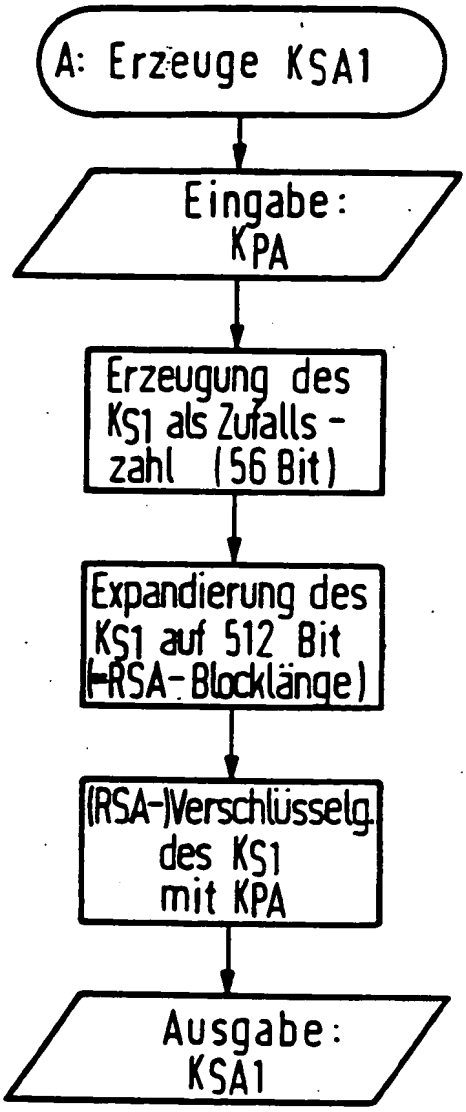


FIG 3



Nummer: DE 38 31 797 C2
Int. Cl.[5]: H 04 L 9/00
Veröffentlichungstag: 22. Oktober 1992

FIG 4

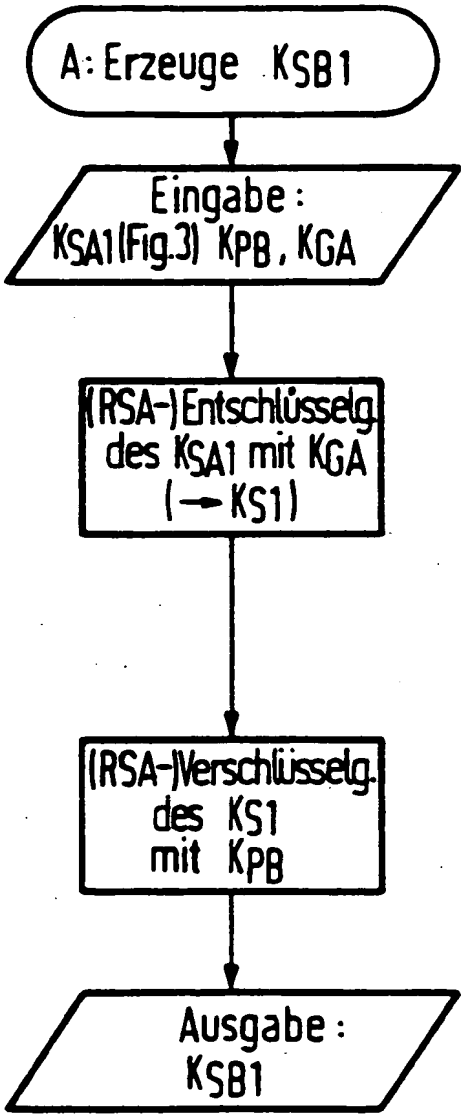
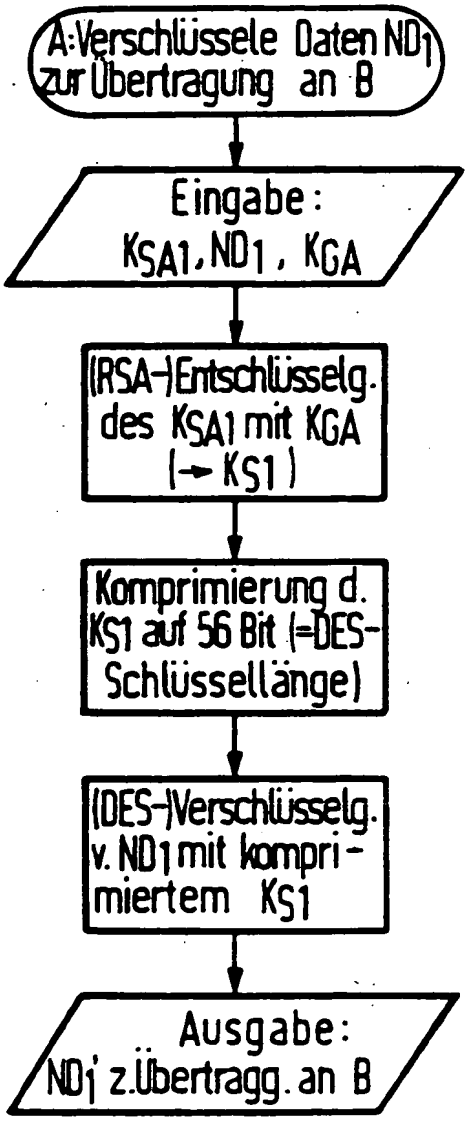
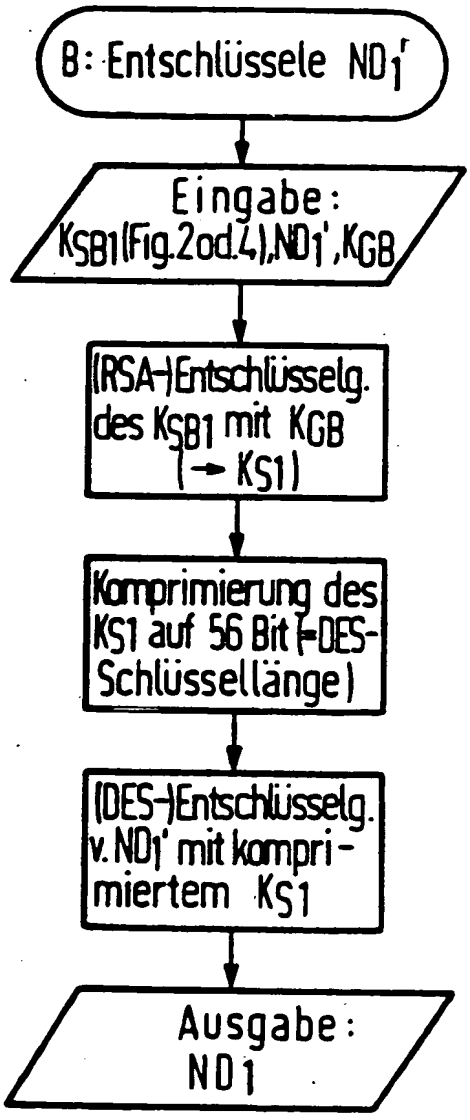


FIG 5



Nummer: DE 36 31 797 C2
Int. Cl.[5]: H 04 L 9/00
Veröffentlichungstag: 22. Oktober 1992

FIG 6



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 36 31 797 C 2**

(51) Int. Cl.[5]:
H 04 L 9/00
G 09 C 1/00

(21) Aktenzeichen: P 36 31 797.7-31
(22) Anmeldetag: 18. 9. 86
(43) Offenlegungstag: 31. 3. 88
(45) Veröffentlichungstag der Patenterteilung: 22. 10. 92

DE 36 31 797 C 2

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Siemens AG, 1000 Berlin und 8000 München, DE

(72) Erfinder:
Schmidtke, Frank, 8000 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US-Z.: ZIMMERMANN, P: A proposed standard format for RSA crypto-systems. In: Computer, Nr. 9, Sept. 1986, S. 21-34;
DE-B.: WECK, G.: Datensicherheit, Stuttgart, B.G. Teubner, 1984, S. 290-295;

(54) Verfahren und Vorrichtung zur Verschlüsselung von Nutzdaten

DE 36 31 797 C 2

Dieses Kommunikationssystem besteht aus mindestens einer Verbindungsleitung und kann neben den beiden Kommunikationsendstellen A und B weitere in Fig. 1 nicht dargestellte Kommunikationsendstellen miteinander verbinden.

Jede Kommunikationsendstelle A und B besteht aus einer räumlich abgeschlossenen Verschlüsselungseinrichtung VA, VB und aus einer an die Verbindungsleitung angeschlossenen Bedienungseinrichtung TA, TB.

Die Verschlüsselungseinrichtung VA der ersten Kommunikationsendstelle A und die Verschlüsselungseinrichtung VB der zweiten Kommunikationsendstelle weisen mindestens eine erste Eingabeeinrichtung AWL_A, AWL_B zur beispielsweise manuellen Eingabe des der jeweiligen Kommunikationsendstelle A beziehungsweise B zugeordneten, aus einem geheimen Schlüssel K_{GA} beziehungsweise K_{GB} und einem öffentlichen Schlüssel K_{PA}, K_{PB} bestehenden Schlüsselpaars auf.

Die geheimen Schlüssel K_{GA} und K_{GB} können auch auf Ausweisen beziehungsweise Chipkarten abgespeichert sein. Zusätzlich können darauf auch die jeweiligen öffentlichen Schlüssel K_{PA}, K_{PB} abgespeichert sein. Die erste Eingabeeinrichtung AWL_A beziehungsweise AWL_B ist dann als Ausweis- beziehungsweise Chipkartenlesegerät ausgebildet.

Die jeweiligen geheimen Schlüssel K_{GA} und K_{GB} können auch in besonderen Speichereinrichtungen in der jeweiligen Verschlüsselungseinrichtung VA oder VB abgespeichert sein, zum Beispiel in Form von steckbaren "Read Only Memories".

Die den beiden Kommunikationsendstellen A und B zugeordneten Schlüsselpaare K_{GA}, K_{PA}; K_{GB}, K_{PB} können aus Sicherheitsgründen jeweils eine zeitlich begrenzte Gültigkeit besitzen.

Zur Eingabe des öffentlichen Schlüssels (z. B. K_{PB}, K_{PA}) derjenigen Kommunikationsendstellen (z. B. B, A), an die Nutzdaten übertragen werden sollen, kann, wenn der betreffende öffentliche Schlüssel einem Verzeichnis entnehmbar ist, die die Nutzdaten absendende Kommunikationsendstelle (z. B. A, B) eine zweite Eingabeeinrichtung EG_A beziehungsweise EG_B aufweisen, die als alphanumerische Eingabeeinrichtung ausgebildet ist. Ist die erste Eingabeeinrichtung AWL_A beziehungsweise AWL_B alphanumerisch ausgebildet, so erübrigt sich die zweite Eingabeeinrichtung EG_A beziehungsweise EG_B. Die zweite Eingabeeinrichtung EG_A beziehungsweise EG_B erübrigt sich auch, wenn der öffentliche Schlüssel (z. B. K_{PB}, K_{PA}) an diejenige Kommunikationsendstelle (z. B. A, B) über die Verbindungsleitung übertragen wird, die die Nutzdaten verschlüsselt, um diese anschließend an die Kommunikationsendstelle (z. B. B, A) zu übertragen, der der übertragene öffentliche Schlüssel (K_{PB}, K_{PA}) zugeordnet ist.

Die öffentlichen Schlüssel K_{PA}, K_{PB} können auch über gesonderte, unten noch beschriebene Eingabeeinrichtungen E/A_A, E/A_B in den Bedieneinrichtungen TA, TB eingegeben werden und gelangen von dort, beziehungsweise von den ebenfalls in TA, TB angeordneten Speichern SP_A, SP_B über die entsprechende Schnittstellenschaltung IF_A, IF_B zur weiteren Bearbeitung in die Verschlüsselungseinrichtung VA beziehungsweise VB.

Die ersten und zweiten Eingabeeinrichtungen AWL_A, AWL_B und EG_A, EG_B sind jeweils mit einer zentralen Steuerung ZST_A, ZST_B verbunden, die wie in Fig. 1 dargestellt in den Verschlüsselungseinrichtungen VA, VB angeordnet sind und mit den Komponenten ZG_A, $E_{A,RSA}$, $D_{A,RSA}$ und IF_A beziehungsweise ZG_B, $D_{B,RSA}$, $E_{B,RSA}$ und IF_B von VA beziehungsweise VB in Verbindung steht.

Der Zufallsgenerator ZG_A in der Verschlüsselungseinrichtung VA der Kommunikationsendstelle A dient der Erzeugung der an der Kommunikation beteiligten Kommunikationsendstellen gemeinsamen temporären Schlüssel als Zufallszahlen K_{S1}, K_{S3}. Die Verschlüsselungseinrichtung VA enthält ferner eine Schnittstellenschaltung IF_A sowie ein nach einem asymmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul $E_{A,RSA}$ sowie ein nach einem asymmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{A,RSA}$. Die vier letztgenannten Komponenten ZG_A, IF_A, $E_{A,RSA}$ und $D_{A,RSA}$ werden von der zentralen Steuerung ZST_A der Kommunikationsendstelle A gesteuert. Das Entschlüsselungsmodul $D_{A,RSA}$ steht außerdem mit einem ebenfalls in der Verschlüsselungseinrichtung VA der Kommunikationsendstelle A angeordneten Verschlüsselungsmodul $E_{A,DES}$ in Verbindung. Diesem Modul werden erste Nutzdaten ND_1 zugeführt, die nach Durchführung eines symmetrischen Verschlüsselungsvorgangs ausgangsseitig als verschlüsselte Nutzdaten ND_1' über die Schnittstellenschaltung IF_A, der Bedieneinrichtung TA und die Verbindungsleitung an die zweite Kommunikationsendstelle B abgegeben werden. Die Module $E_{A,DES}$ und $D_{A,DES}$ können auch unmittelbar an die zentrale Steuerung ZST_A angeschlossen sein, so daß die Ausgangsparameter der Module $D_{A,RSA}$ und $E_{A,RSA}$ den Modulen $E_{A,DES}$ und $D_{A,DES}$ über die zentrale Steuerung ZST_A zugeführt werden.

Die zweite Kommunikationsendstelle B weist zur Durchführung des Verfahrens nach Anspruch 1 neben der Bedieneinrichtung TB in der zugeordneten Verschlüsselungseinrichtung VB die Komponenten ZST_B, AWL_B, gegebenenfalls EG_B, ein nach einem asymmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{B,RSA}$ und ein mit diesem in Verbindung stehendes, nach einem symmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{B,DES}$ auf. Dieses Entschlüsselungsmodul $D_{B,DES}$ entschlüsselt die von der ersten Kommunikationsendstelle A übertragenen verschlüsselten ersten Nutzdaten ND_1' nach einem symmetrischen Verschlüsselungsverfahren und erzeugt wieder die Originalnutzdaten ND_1.

Die zweite Kommunikationsendstelle B kann so ausgebildet sein, daß sie nicht nur von der ersten Kommunikationsendstelle A erste verschlüsselte und übertragene Nutzdaten ND_1 entschlüsselt, sondern ihrerseits zweite Nutzdaten ND_2 verschlüsselt und die zweiten verschlüsselten Nutzdaten ND_2' an die erste Kommunikationsendstelle A überträgt. Dabei kann, wie weiter unten näher erläutert wird, die Verschlüsselung der zweiten Nutzdaten ND_2 in der zweiten Kommunikationsendstelle B mittels eines von der ersten Kommunikationsendstelle A erzeugten Schlüssel K_{SB1} oder mittels eines in der zweiten Kommunikationsendstelle B erzeugten Schlüssels K_{SB2} erfolgen.

Verschlüsselt die zweite Kommunikationsendstelle B zweite Nutzdaten ND_2, so enthält ihre Verschlüsselungseinrichtung VB ein nach einem symmetrischen Verschlüsselungsverfahren arbeitendes Verschlüsselungsmodul $E_{B,DES}$, während die Verschlüsselungseinrichtung VA der ersten Kommunikationseinrichtung A ein nach dem symmetrischen Verschlüsselungsverfahren arbeitendes Entschlüsselungsmodul $D_{A,DES}$ zur Entschlüsselung der zweiten verschlüsselten, von der ersten Kommunikationsendstelle A übertragenen Nutzdaten

den. Dies geschieht beispielsweise dadurch, indem an K_{S1} Bitfolgen angehängt werden, die nach einer vorgegebenen festen Regel gebildet werden. Beispielsweise werden die angehängten Bitfolgen aus K_{S1} abgeleitet. Die Expandierung beziehungsweise eine spätere Komprimierung (Fig. 5, 6) ist notwendig, wenn die beiden beim erfindungsgemäßen Verfahren benutzten Verschlüsselungsverfahren, ein asymmetrisches Verfahren, insbesondere das RSA-Verfahren, und ein symmetrisches Verfahren, insbesondere das DES-Verfahren blockorientiert, das heißt stets mit ganzzahlig Vielfachen der Blocklänge arbeiten.

Als praktikabel im Hinblick auf Sicherheit und Realisierung hat sich für das RSA-Verfahren eine Blocklänge von 512 Bit erwiesen, während das standardisierte DES-Verfahren mit einer Blocklänge von 64 Bit arbeitet.

Der vom Zufallsgenerator ZG_A erzeugte Schlüssel K_{S1} wird erfindungsgemäß nach einem asymmetrischen Verschlüsselungsverfahren, insbesondere nach dem RSA-Verschlüsselungsverfahren, verschlüsselt. Diese Verschlüsselung erfolgt mit Hilfe des Verschlüsselungsmoduls $E_{A,RSA}$ dem die öffentlichen Schlüssel K_{PA1} und K_{PB1} zugeführt werden. Die Verschlüsselung des expandierten ersten temporären Schlüssels K_{S1} liefert einen ersten temporären Schlüssel K_{SA1} und einen zweiten temporären Schlüssel K_{SB1}, der von der ersten Kommunikationsendstelle A mittels der zentralen Steuerung ZST_A über die Schnittstellenschaltung IF_A, die Bedieneinrichtung TA und die Verbindungsleitung an die zweite Kommunikationsendstelle B übertragen wird. Dieser an B zu übertragende Schlüssel K_{SB1}, der der späteren Entschlüsselung der ersten Nutzdaten ND_1' dient, kann unverschlüsselt oder verschlüsselt, übertragen werden. Die Verschlüsselung des zu übertragenden K_{SB1} kann beispielsweise auch nach dem erfindungsgemäßen Verfahren erfolgen. Hierzu wird beiden Kommunikationsendstellen A und B jeweils ein Schlüssel K_{SA0}, K_{SB0} fest zugeordnet, der von der jeweiligen Verschlüsselungseinrichtung VA beziehungsweise VB zu einem beiden Endstellen A und B gemeinsamen Schlüssel K_{S0} verarbeitet wird. K_{SA0}, K_{SB0} werden nur für die Ver- und Entschlüsselung des zu übertragenden K_{SB1} verwendet. Damit lassen sich Schlüsselhierarchien realisieren, bei denen in den Endstellen nur individuelle, übergeordnete Schlüssel (K_{SA0}, K_{SB0}), nicht jedoch identische Schlüssel (K_{S0}) wie im Stand der Technik abgespeichert werden.

Fig. 2 zeigt die gleichzeitige Erzeugung der beiden Schlüssel K_{SA1} und K_{SB1}. Beide Schlüssel können, wie in Fig. 3 dargestellt, jedoch auch zeitlich versetzt, aber in sonst gleicher Weise erzeugt werden. Dies geschieht in den folgenden Schritten: Erzeugung von K_{S1}, Expandierung, Verschlüsselung des expandierten K_{S1} mit dem öffentlichen Schlüssel K_{PA}, damit Bildung des ersten temporären Schlüssels K_{SA1} (Fig. 3); Verschlüsselung des expandierten K_{S1} mit dem öffentlichen Schlüssel K_{PB}, damit Bildung des zweiten temporären Schlüssels K_{SB1}.

Die separate Bildung des ersten temporären Schlüssels K_{SA1} ermöglicht eine Bildung des zweiten temporären Schlüssels K_{SB1} nach Fig. 4. Die zentrale Steuerung ZST_A führt dem nach einem asymmetrischen Verfahren, insbesondere nach dem RSA-Verfahren arbeitenden Entschlüsselungsmodul $D_{A,RSA}$ den ersten temporären Schlüssel K_{SA1} sowie den geheimen oder privaten Schlüssel K_{GA} zu. $D_{A,RSA}$ liefert K_{S1}, den beiden Kommunikationsstellen A, B gemeinsamen Schlüssel, der aber aus Sicherheitsgründen die Verschlüsselungseinrichtung VA nicht verläßt. Vom Ausgang des Entschlüsselungsmoduls $D_{A,RSA}$ wird K_{S1} über die zentrale Steuerung ZST_A zusammen mit dem öffentlichen Schlüssel K_{PB} an das nach einem asymmetrischen Verfahren, insbesondere nach dem RSA-Verfahren arbeitende Verschlüsselungsmodul $E_{A,RSA}$ geschaltet, Das K_{SB1} erzeugt. K_{SB1} wird wie Fig. 1 zeigt mittels der zentralen Steuerung ZST_A über die Schnittstellenschaltung IF_A, die Bedieneinrichtungen TA und TB der Verschlüsselungseinrichtung VB zugeführt.

Fig. 5 veranschaulicht den Teil des Verfahrens gemäß der Erfindung, in dem die Verschlüsselung der Nutzdaten ND_1 in VA erfolgt. Der erste temporäre Schlüssel K_{SA1}, der im ersten Verfahrensabschnitt in der ersten Kommunikationsendstelle A entsprechend Fig. 2 oder Fig. 3 erzeugt wurde und in dem in der Bedieneinrichtung TA angeordneten Speicher SP_A zwischengespeichert werden kann, wird mit dem beispielsweise über die erste Eingabeeinrichtung AWL_A einzugebenden privaten (RSA-)Schlüssel K_{GA} entschlüsselt und dabei wird ein beiden Kommunikationsendstellen A und B gemeinsamer erster temporärer Schlüssel K_{S1} mittels des Entschlüsselungsmoduls $D_{A,RSA}$ gebildet. Der auf diese Weise gebildete Schlüssel dient der Verschlüsselung der ersten Nutzdaten ND_1 nach einem symmetrischen Verschlüsselungsverfahren, insbesondere nach dem DES-Verschlüsselungsverfahren. Vor der DES-Verschlüsselung wird der erste temporäre Schlüssel auf die DES-Schlüssellänge von 56 Bit komprimiert. Die ersten Nutzdaten ND_1, die der Kommunikationsendstelle A von einer externen Datenquelle zugeführt oder beispielsweise mittels der in der Bedieneinrichtung TA angeordneten Eingabeeinrichtung E/A_A erzeugt werden können, werden in der Verschlüsselungseinrichtung VA über die Schnittstellenschaltung IF_A mittels der zentralen Steuerung ZST_A an den Eingang des Verschlüsselungsmoduls $E_{A,DES}$ durchgeschaltet. Das Ergebnis der DES-Verschlüsselung der Daten ND_1 mit dem komprimierten ersten temporären Schlüssel K_{S1} liefert verschlüsselte Daten ND_1', die über die Schnittstellenschaltung IF_A und die Bedieneinrichtung TA an die zweite Kommunikationsendstelle B zur dortigen Entschlüsselung übertragen werden.

Über die Verbindungsleitung werden zwischen den Kommunikationsendstellen A und B also der zweite temporäre (RSA-)Schlüssel K_{SB1} und die (DES-) verschlüsselten Nutzdaten ND_1' übertragen. Der zweite temporäre (RSA-)Schlüssel K_{SB1} ist nur durch den geheimen, der Kommunikationsendstelle B zugeordneten (RSA-)Schlüssel K_{GB} entschlüsselbar. Die (DES-) verschlüsselten Nutzdaten ND_1' sind nur mit dem beiden Kommunikationsendstellen A, B gemeinsamen (DES-)Schlüssel K_{S1} entschlüsselbar, der in der Verschlüsselungseinheit VB aus dem zweiten temporären (RSA-)Schlüssel K_{S1} mit Hilfe des geheimen Schlüssels K_{GB} erzeugt wird.

Fig. 6 veranschaulicht den abschließenden Abschnitt des Verfahrens gemäß der Erfindung, bei dem die von A übertragenen ersten verschlüsselten Nutzdaten ND_1' in VB entschlüsselt werden. Der von der ersten Kommunikationsendstelle A übertragene zweite temporäre Schlüssel K_{SB1}, der im Speicher SP_B der Bedieneinrichtung TB zwischenspeicherbar ist, wird mit Hilfe der zentralen Steuerung ZST_B über die Schnittstellenschaltung IF_B dem Entschlüsselungsmodul $D_{B,RSA}$ zugeführt und mit dem beispielsweise über die erste Eingabeeinrichtung AWL_B einzugebenden privaten (RSA-)Schlüssel K_{GB} entschlüsselt. Das Ergebnis dieses Entschlüsselungsvorgangs ist der beiden Kommunikationsendstel-